ABSTRACT OF THE DISCLOSURE

A system and method to support platform firmware as a trusted process. Measurement of a trusted portion of original firmware are measured by a core root of trust measurement (CRTM). The measurement is stored in a secure manner during pre-boot. During operating system (OS)-runtime, requests are made to access an unqualified current version of firmware corresponding to a secure execution mode. A portion of the current firmware analogous to the trusted portion is measured. The measurements of the trusted original portion and unqualified current portion are compared to verify they match. If they match, it indicates that the current portion and the trusted portion are one in the same. Thus, the current portion of firmware is trustworthy. Accordingly, the firmware may be executed as a trusted process. Embodiments employ locality to enforce the trusted process. The use of locality prevents unqualified users (*i.e.*, software) from accessing data stored by trusted firmware.